CMPS 455 Project 2

Jacob Tilmon	C00292879
Amy Canelas	C00416506
Ruby Shrestha	C00451990
Jessica Espree	C00081195

As part of your report, answer the following question about Task 1:

1. **Is there any chance of deadlock in this simulation? What changes could cause deadlocks?**

No, there isn't a chance of deadlock in this simulation. The changes that could cause a deadlock would be if we implemented it as a readers writers problem.

As part of your report, answer the following questions about Task 2:

1. **How does this task compare with Task 1? Which is easier to implement?**

The logic to generate our access list, creates threads and access to objects remains similar to task 1. Unlike task 1, we are not storing null entries and therefore this approach is more optimal when it comes to memory allocation. In both tasks, the threads remain represented by the user (not a domain nor an object). Yet in Task 2, we are using an arraylist of arraylist type String, to simulate a list of access rights and authorization to domain switch per each randomly generated object (upper bound of M). Each access right pertains to a domain number, so if there are three access rights displayed, then there are three domains. Following the three access rights, will be alternating "-" or "allow", that will signify if a domain is allowed to switch.

In our opinion, they are relatively the same, but the access matrix is simpler due to the fact that the programmer does not have to deal with omitting null entries. It is as simple as generating the contents for the matrix with no consideration to how the block of memory allocated will be used.

As part of your report, answer the following questions about Task 3:

1. **What disadvantages do capability lists introduce given a more domain-based approach?**

   Capability lists forces a limited number of users type; meaning the user roles can only be equal to the amount of the domains

Task 5: Report
What is the importance of protection in a multi-user system?
What could happen if all users were granted equal permission?

- Access rights
  - You wouldn't want all users access to sensitive information such as banking information and social security numbers.
- Accidental data exposure.
  - If users are not aware of proper cybersecurity rules, it could lead to accidental data and resource leak. An user might not have ill intention but he simply could be ignorant to not know the power of his access right
- Intentional access misuse
  - Users might intentionally misuse their access, which will result leaking and theft of resources
- Compromise of system
  - If all users have the same access to the system, it is easier for hackers to crack into the system. They will have access to entire system even if they break one user’s credentials
- Defeats the advantages of authorization rights since everyone would have the same clearance, therefore it would be inaccurate.

.